Exhibit I

RIDGEVIEW MEDICAL CENTER AND CLINICS **#3516**

SUBJECT: PASSWORDS POLICY

ORIGINATING DEPT: Information Technology (IT) **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12
Revision Dates:

Reviewed Dates:

APPROVAL:
Administration: ____________________

Director: ____________________

PURPOSE:

The purpose of the Ridgeview Medical Center Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of Ridgeview Medical Center user authentication mechanisms.

Audience

The Ridgeview Medical Center Password Policy applies equally to all individuals who use any Ridgeview Medical Center Information Resource.

POLICY:

- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Ridgeview Medical Center rules:
  - Must be routinely changed
  - Must adhere to the minimum length of eight (8) characters, as established by Ridgeview Medical Center IS Management
  - Must be a combination of alpha and numeric and special characters
  - Must not be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
  - Must not be dictionary words or acronyms
- Password history must be kept to prevent the reuse of passwords
- Stored passwords are classified as Confidential Data and must be encrypted
- User account passwords must not be divulged to anyone. Ridgeview Medical Center support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Ridgeview Medical Center, if issued.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators/Special Access users must not circumvent the Ridgeview Medical Center Password Policy for the sake of ease of use.
- Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Ridgeview Medical Center Information Security Committee. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

- Ridgeview Medical Center IS Support password change procedures must include the following:
  - Authenticate the user to the helpdesk before changing password
  - Change to a strong password
  - The user must change password at first login
- The unauthorized disclosure of a password constitutes an incident in which the proper incident management procedures must be followed
- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the account and password(s)
  - Report the discovery to Ridgeview Medical Center IS Support

WAIVERS:
Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 – Enterprise Information Security Governance.

ENFORCEMENT:
Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.